

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-82834

(P2002-82834A)

(43) 公開日 平成14年3月22日 (2002.3.22)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 A 5 B 0 1 7
11/34		11/34	C 5 B 0 3 5
G 0 6 K 19/00		G 0 9 C 1/00	6 4 0 B 5 B 0 4 2
19/10		G 0 6 K 19/00	Q 5 J 1 0 4
G 0 9 C 1/00	6 4 0		R

審査請求 未請求 請求項の数 6 O L (全 14 頁)

(21) 出願番号 特願2000-271904(P2000-271904)

(22) 出願日 平成12年9月7日(2000.9.7)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 西澤 秀和

東京都府中市東芝町1番地 株式会社東芝  
府中事業所内

(72) 発明者 加藤 岳久

東京都府中市東芝町1番地 株式会社東芝  
府中事業所内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

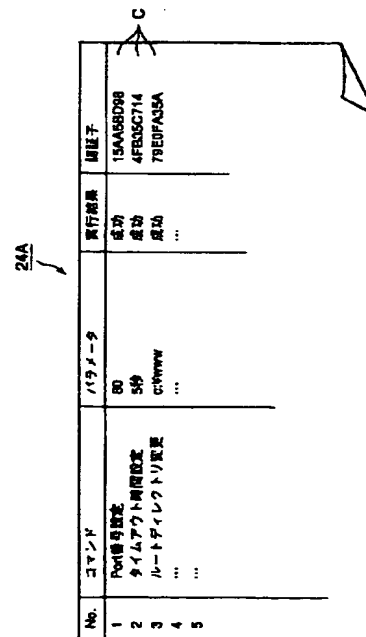
最終頁に続く

(54) 【発明の名称】 履歴管理用の記憶媒体及びICカード

(57) 【要約】

【課題】 管理者による履歴の改ざんを阻止する。

【解決手段】 管理者の操作履歴に対して各履歴データ毎に認証子Cをつけるので、履歴データが改ざんされていない旨と、個々の履歴データの連鎖性を保証する。また、最新の認証子Cの比較結果をも検証するので、最新の履歴データが削除されていない旨をも保証する。



## 【特許請求の範囲】

【請求項1】 計算機システムの操作の履歴管理を実現するための履歴管理用のコンピュータ読取り可能な記憶媒体であって、

前記計算機システムのコンピュータを、  
前記操作毎に今回の履歴データ及び認証子が追加的に記憶される履歴テーブルを形成するテーブル形成手段、  
前記操作毎に今回の履歴データ及び前回の認証子に基づいて今回の認証子が生成されると、この今回の認証子を前記今回の履歴データと組にして前記履歴テーブルに記憶させる履歴管理手段、  
として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体。

【請求項2】 請求項1に記載のコンピュータ読取り可能な記憶媒体において、

前記計算機システムのコンピュータを、  
前記履歴テーブル内の各回の履歴データ毎に、当該回の履歴データと当該回の前回の認証子とに基づいて、当該回の認証子が生成されるか否かを定期的に検証する第1の検証手段、  
前記第2の検証手段により当該回の認証子が生成されな  
いとき、警告を発する第1の警告手段、  
として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体。

【請求項3】 請求項2に記載のコンピュータ読取り可能な記憶媒体において、

前記計算機システムのコンピュータを、  
前記履歴テーブル内の最新の認証子を比較のために出力し、折り返し入力された比較結果を判定する第2の検証手段、  
前記第2の検証手段による判定結果が不整合を示すとき、警告を発する第2の警告手段、  
として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体。

【請求項4】 請求項3に記載のコンピュータ読取り可能な記憶媒体において、

前記第2の検証手段は、ログオンのときに動作することを特徴とするコンピュータ読取り可能な記憶媒体。

【請求項5】 電子計算機システムの操作の履歴管理を実現するための履歴管理用のICカードであって、耐タンパー性を有し、最新の認証子が記憶される最新認証子記憶手段と、

前記操作毎に今回の履歴データが入力されると、今回の履歴データと前記最新認証子記憶手段内の最新の認証子とに基づいて、今回の認証子を生成する認証子生成手段と、  
この認証子生成手段により生成された今回の認証子を最新の認証子として前記最新認証子記憶手段に書込む認証子書込手段と、

認証子が入力されたとき、この入力された認証子と、前

記最新認証子記憶手段内の最新の認証子とを比較し、比較結果を出力する認証子比較手段と、  
を備えたことを特徴とするICカード。

【請求項6】 請求項5に記載のICカードにおいて、パスワードによる操作者の認証を実行する操作者認証手段を備え、

前記認証子比較手段は、前記操作者認証手段による認証結果が正当なとき、動作することを特徴とするICカード。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、計算機システムの操作の履歴管理を実現するための履歴管理用の記憶媒体及びICカードに係り、特に、管理者による履歴の改ざんを阻止し得る履歴管理用の記憶媒体及びICカードに関する。

## 【0002】

【従来の技術】従来、計算機システムでは、個人のファイルの覗き見又は改変等の不正アクセスや、ネットワーク設定等の不正な改変といった様々な不正操作を阻止する観点から、履歴管理用のプログラムがインストールされて実行されている。図14はこの種の計算機システムの概略を示す模式図であり、図15はこの計算機システムの構成を示す機能ブロック図である。

【0003】この計算機システムは、計算機10とサーバ装置20とがネットワークNWを介して接続され、サーバ装置20には管理操作用のコンソール10\*が接続されている。但し、コンソール10\*と計算機10とは基本的に同一構成であり、ネットワークを介するか否かの違いしかないので、以後の説明では、コンソール10\*からの管理操作の記載を省略し、計算機10からの管理操作を例に挙げて述べる。

【0004】一般に、計算機10は任意の部屋に設置されるが、サーバ装置20は、物理的な脅威から保護されるように、計算機10の部屋とは異なる安全な部屋に設置される。システム管理者は、システムの全操作を実行可能な権限を有し、計算機10をネットワークNW経由でサーバ装置20に接続して管理操作を行なう。

【0005】ここで、計算機10は、例えばパーソナルコンピュータ(PC)等が使用可能であり、サーバ装置20のソフトウェアを遠隔管理するための管理ソフトウェアがインストールされている。計算機10は、具体的には図15に示すように、システム管理者の管理操作用の視覚的ツールであるGUI(Graphical User Interface)11と、システム管理者によるGUI11の操作に基づき管理用のコマンド電文を作成するコマンド発行機能12と、この作成されたコマンド電文をネットワークNW経由でサーバ装置20に送出するソケット13とがインストールされている。

【0006】サーバ装置20は、サービスを提供するソ

ソフトウェアがインストールされて稼働しており、具体的には、計算機10からのコマンド電文を受け取るソケット21と、この受け取ったコマンド電文を解釈するコマンド解釈機能22と、コマンド電文を解釈したコマンド解釈機能22に制御され、サーバ装置20の各種の管理をコマンド電文に応じて個別に実行する複数の管理機能23(A, B, C, ...)とがインストールされ、コマンド解釈機能22により、管理機能23にて実行された管理操作の履歴が記録される履歴テーブル24が形成されて使用されている。

【0007】ここで、履歴テーブル24は、図16に一例を示すように、個々の管理操作(コマンド電文)に対応して各行毎に、No. (連番の番号)、コマンド(操作内容)、パラメータ及び実行結果(成功又は失敗)が記録された表形式の記憶領域である。この履歴テーブル24の参照により、システム管理者による管理操作は、その実行順序に沿って履歴管理されている。

【0008】

【発明が解決しようとする課題】しかしながら以上のような履歴管理では、第三者に対しては不正操作の痕跡を記録することから不正操作を阻止し得るものの、システム管理者に対しては不正操作の痕跡が消去可能であることから不正操作を阻止し得ない状況にある。

【0009】詳しくは、システム管理者は、計算機システムの全操作の権限を持つため、不正操作が履歴テーブル24に記録されても、自己の操作権限により、履歴テーブル24を改ざんして不正操作の痕跡を消去可能であるからである。

【0010】なお、履歴テーブル24の改ざん内容としては、次の(1)～(5)に示す5種類又はこれらの組合せが考えられる。

- (1) 履歴の1行(最新の履歴を除く)を削除
- (2) 履歴テーブルの最新の履歴を削除
- (3) 履歴の1行について改変
- (4) 虚偽の履歴を途中の行の間に挿入
- (5) 虚偽の履歴を最新の行の後に追加

一方、このようなシステム管理者による履歴テーブル24の改ざんを不可能とする観点から、システム全体の操作権限を分割する場合がある。この場合、システム操作の権限をもつ管理者と、ネットワーク操作やアプリケーション操作の権限をもつ管理者とを異なる人物に担当させている。しかしながら、この場合でも管理者同士の結託により、履歴テーブル24が改ざんされる可能性がある。

【0011】従って、たとえ履歴テーブル24の操作権限を持つ管理者であっても、履歴テーブル24の改ざんを不可能とする技術が必要とされている。

【0012】本発明は上記実情を考慮してなされたもので、管理者による履歴の改ざんを阻止し得る履歴管理用の記憶媒体及びICカードを提供することを目的とする。

る。

【0013】

【課題を解決するための手段】第1の発明は、計算機システムの操作の履歴管理を実現するための履歴管理用のコンピュータ読取り可能な記憶媒体であって、前記計算機システムのコンピュータを、前記操作毎に今回の履歴データ及び認証子が追加的に記憶される履歴テーブルを形成するテーブル形成手段、前記操作毎に今回の履歴データ及び前回の認証子に基づいて今回の認証子が生成されると、この今回の認証子を前記今回の履歴データと組にして前記履歴テーブルに記憶させる履歴管理手段、として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体である。ここで、履歴データは、例えばコマンド、パラメータ及び実行結果の組であり、所望によって以上の組に行番号を含めてもよい。

【0014】このように、管理者の操作履歴に対する各履歴データ毎に、前回の認証子をも含んで生成した認証子をつけるので、履歴データが改ざんされていない旨と、個々の履歴データの連鎖性を保証でき、もって、管理者による履歴の改ざんを阻止することができる。

【0015】第2の発明は、第1の発明において、前記計算機システムのコンピュータを、前記履歴テーブル内の各回の履歴データ毎に、当該回の履歴データと当該回の前回の認証子とに基づいて、当該回の認証子が生成されるか否かを定期的に検証する第1の検証手段、前記第2の検証手段により当該回の認証子が生成されないとき、警告を発する第1の警告手段、として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体である。

【0016】従って、定期的に第1の発明と同様の作用を奏することができる。

【0017】第3の発明は、第2の発明において、前記計算機システムのコンピュータを、前記履歴テーブル内の最新の認証子を比較のために出力し、折り返し入力された比較結果を判定する第2の検証手段、前記第2の検証手段による判定結果が不整合を示すとき、警告を発する第2の警告手段、として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体である。

【0018】このように、最新の認証子の比較結果をも検証するので、第2の発明の作用に加え、最新の認証子の削除に関しても、管理者による履歴の改ざんを阻止することができる。

【0019】第4の発明は、第3の発明において、前記第2の検証手段がログオンのときに動作するコンピュータ読取り可能な記憶媒体である。

【0020】従って、ログオン時に第3の発明と同様の作用を奏することができる。

【0021】一方、第5の発明は、電子計算機システムの操作の履歴管理を実現するための履歴管理用のICカ

ードであって、耐タンパー性を有し、最新の認証子が記憶される最新認証子記憶手段と、前記操作毎に今回の履歴データが入力されると、今回の履歴データと前記最新認証子記憶手段内の最新の認証子とに基づいて、今回の認証子を生成する認証子生成手段と、この認証子生成手段により生成された今回の認証子を最新の認証子として前記最新認証子記憶手段に書込む認証子書込手段と、認証子が入力されたとき、この入力された認証子と、前記最新認証子記憶手段内の最新の認証子とを比較し、比較結果を出力する認証子比較手段と、を備えたICカードである。

【0022】このように、耐タンパー性を有して最新の認証子を保持し、最新の認証子の比較結果を検証するので、最新の履歴に関し、管理者による履歴の改ざんを阻止することができる。

【0023】第6の発明は、第5の発明において、パスワードによる操作者の認証を実行する操作者認証手段を備え、前記認証子比較手段としては、前記操作者認証手段による認証結果が正当なとき、動作するICカードである。

【0024】従って、操作者の認証後に第5の発明と同様の作用を奏することができる。

【0025】

【発明の実施の形態】以下、本発明の各実施形態について図面を参照しながら説明する。

（第1の実施形態）図1は本発明の第1の実施形態に係る記憶媒体内のプログラムがインストールされた計算機システムの概略を示す模式図であり、図2はこの計算機システムの構成を示す機能ブロック図であって、前述した図面と同一部分には同一符号を付し、前述した部分を改良した部分にはアルファベットの添字を付して、前述した部分と重複する説明を省略し、ここでは異なる部分について主に述べる。なお、以下の各実施形態も同様にして重複した説明を省略する。

【0026】すなわち、本実施形態は、管理者による履歴の改ざんを阻止し得るものであり、具体的には、前述の履歴テーブル24に代えて、各行毎に認証子Cをも記憶する履歴テーブル24Aが設けられ、且つこの履歴テーブル24Aとコマンド解釈機能22との間に履歴管理機能25が設けられ、この履歴管理機能25がICカードR/W26を介してICカード30に接続可能な構成となっている。

【0027】ここで、履歴テーブル24Aは、図3に示すように、前述した履歴テーブル24に比べ、各操作に対応するコマンド、パラメータ及び実行結果の組毎に認証子Cが記録される構成となっている。なお、履歴テーブル24Aは、例えば、始めに履歴管理機能25により初期化されて形成される。

【0028】認証子Cは、前回までの行に記憶された履歴データ（例、コマンド、パラメータ及び実行結果の

組）及び認証子Cと、今回の行に記憶された履歴データとに密接に関連するデータであり、例えば署名データのように何らかの暗号化データが適用可能となっている。

【0029】具体的には認証子Cは、前回の行の認証子Cと、今回の行のコマンド、パラメータ及び実行結果とに関してICカード30内で秘密鍵を用いた暗号化処理により生成され、ICカードR/W26及び履歴管理機能25を介して履歴テーブル24Aの該当する行番号の列領域に書込まれる。但し、認証子Cの生成方法は、コマンド、パラメータ、実行結果、直前行の認証子C、及び秘密鍵についての関数であればよく、その生成過程は任意である。

【0030】例えば、今回のコマンド、パラメータ及び実行結果と、直前行の認証子Cとについてのハッシュ値を取り、得られたハッシュ値を秘密鍵で暗号化した値を最新の認証子Cとする生成方法や、今回のコマンド、パラメータ及び実行結果の組のハッシュ値を得た後、このハッシュ値と直前行の認証子Cとの排他的論理和XORを取り、得た結果を秘密鍵で暗号化した値を最新の認証子Cとする生成方法などが考えられる。

【0031】なお、認証子Cは、検証時に、履歴を削除・改変・挿入・追加した内容（1）、（3）～（5）の改ざんを検知する機能として、（f1）一行毎の履歴が改ざんされていない旨を保証する機能と、（f2）直前の認証子Cと関連を有して履歴の連鎖性を保証する機能とを有している。例えば、ある行の履歴を削除した場合、削除した行よりも後の行の認証子Cを検証した際に、エラーを発生させる。

【0032】履歴管理機能25は、コマンド解釈機能22と履歴テーブル24Aとの間に介在して設けられ、最新の認証子Cを更新する更新機能と、認証子の内容を検証する第1の検証機能と、最新の認証子Cの削除を検証する第2の検証機能とを有するものである。履歴管理機能25における更新機能は、コマンド解釈機能22から受けたコマンド、パラメータ及び実行結果をICカードR/W26を介してICカード30に入力し、折り返し、ICカード30から受けた認証子Cと、当該コマンド、パラメータ及び実行結果とを履歴テーブル24Aの最後の同一行に書込むものである。

【0033】履歴管理機能25における第1の検証機能は、履歴テーブル24A内の各行毎に、k行目のコマンド、パラメータ及び実行結果と、k-1行目の認証子Cとを対象にし、公開鍵を用いて認証子Cの生成と逆の操作により、k行目の認証子Cを検証するものである。

【0034】一方、ICカード30は、図4に示すように、最新認証子格納庫31、秘密鍵格納庫32及び制御機能33を備えている。履歴管理機能25における第2の検証機能は、履歴テーブル10の最新の行の認証子Cを読出してこの認証子CをICカードR/W26経由で制御機能33に送る一方、制御機能33から返信された

比較結果を判定するものである。

【0035】なお、履歴管理機能25は、ハードウェア及び／又はソフトウェアにより実現可能であり、ソフトウェアで実現される場合、コンピュータ読取り可能な記憶媒体から履歴管理機能25に相当するプログラムがインストールされて実現される。これは他の各機能21～23についても同様である。

【0036】最新認証子格納庫31は、耐タンパー性を有し、外部から一切アクセス不能であって常に最新の認証子Cが追加又は更新されて格納される領域であり、制御機能33により最新の認証子Cが読出／書込可能となっている。なお、最新認証子格納庫31は、最新の行の履歴に対する認証子Cを外部から改変不可に保持することにより、履歴テーブル24Aにおける最新の履歴を削除する内容(2)の改ざんを阻止する機能(又は改ざん後にそれを検出する機能)を有する。また、最新認証子格納庫31の認証子Cは、初めてICカード30により管理操作を行う場合には予め定められた初期値Cが設定され、以後、新たな認証子Cが生成される毎に、最新の認証子Cに書換えられる。

【0037】秘密鍵格納庫32は、耐タンパー性を有し、外部から一切アクセス不能であってICカード30の秘密鍵が格納される領域であり、制御機能33により読出可能となっている。

【0038】制御機能33は、最新の認証子を更新する更新機能と、最新の認証子を検証する検証機能とを有する。制御機能33における更新機能は、履歴管理機能25からICカードR/W26を介して、コマンド、パラメータ及び実行結果からなる今回の処理内容を受けたとき、この処理内容を秘密鍵格納庫31内の秘密鍵で暗号化し、得られた最新の認証子Cを最新認証子格納庫31に書込む一方、この最新の認証子CをICカードR/W26を介して履歴管理機能25に返信するものである。

【0039】制御機能33における検証機能は、履歴管理機能25からICカードR/W26を介して受信した認証子Cと、最新認証子格納庫31内の最新の認証子Cとを比較し、両者の比較結果をICカードR/W26を介して履歴管理機能26に返信するものである。

【0040】次に、以上のように構成された計算機システムの動作を図5～図7のフローチャートを用いて説明する。

(管理操作) 計算機10は、図5に示すように、管理者の操作により、GUI11により操作内容を指定する(ST1)。

【0041】この操作内容は、コマンド発行機能12によりコマンドとパラメータとを含む形式のコマンド電文に変換され、このコマンド電文がソケット13を経由してサーバ装置20Aに送信される(ST2)。

【0042】サーバ装置20Aでは、コマンド電文がソケット21を経由してコマンド解釈機能22に入力さ

れ、コマンド解釈機能22によりコマンド電文からコマンドとパラメータが取り出される(ST3)。

【0043】また、コマンド解釈機能22は、コマンドに対応する管理機能23を実行し、実行結果を管理機能23から受け取る(ST4)。

【0044】次に、コマンド解釈機能22は、コマンド、パラメータ及び実行結果を履歴管理機能25に入力する(ST5)。履歴管理機能25は、コマンド、パラメータ及び実行結果をICカードR/W26を経てICカード30に入力する(ST6)。

【0045】ICカード30では、制御機能33が、これら入力された今回のコマンド、パラメータ及び実行結果と、最新認証子格納庫31の前の認証子Cとに対し、秘密鍵格納庫32内の秘密鍵による暗号化を施して最新の認証子Cを生成する(ST7)。

【0046】ICカード30は、最新の認証子Cを最新認証子格納庫31に格納し(ST8)、この最新の認証子CをICカードR/W26を通して履歴管理機能25に返す(ST9)。履歴管理機能25は、コマンド、パラメータ及び実行結果と最新の認証子Cとを履歴テーブル24Aに書込む(ST10)。

【0047】履歴テーブル24Aへの書込完了後、コマンド解釈機能22は、実行結果を計算機10に返すためのレスポンス電文を生成し、ソケット21を経由して計算機10に返信する(ST11)。

【0048】計算機10は、このレスポンス電文を受信し、GUI11により実行結果を表示して今回の操作を終了する(ST12)。

【0049】(履歴の検証) 以上のように記録された履歴テーブル24Aは、履歴管理機能25による認証子Cの検証により、履歴の改ざんの有無が定期的に調べられる。なお、検証の際には、履歴テーブル24Aの各行毎に認証子Cが正当(=各行の連鎖及び生成が正当)であるか否かの履歴の検証と、最新の認証子CとICカード内の認証子Cとが同一であるか否かの最新履歴の検証とが実行される。以下、詳しく説明する。

【0050】始めに、履歴管理機能25は、図6に示すように、履歴テーブル24A内の行番号kを定め、k=1とする(ST21)。次に、履歴管理機能25は、履歴テーブル24Aのk行目のコマンド、パラメータ、実行結果及び認証子Cを読み出し(ST22)、行番号k=1であるか否かを判定する(ST23)。

【0051】行番号k=1の場合には、履歴テーブル24A内のk-1行目が無いため、直前行の認証子Cとして予め定めた初期値を入れる(ST24)。

【0052】行番号k≠1の場合には、履歴テーブル24A内のk-1行目の認証子Cを読み出す(ST25)。

【0053】ステップST24又はST25の後、k行目のコマンド、パラメータ及び実行結果と、k-1行目

の認証子Cと、公開鍵とを用いてk行目の認証子Cを検証する(ST26)。この検証は、認証子Cの生成方法と逆の操作で実行可能であり、その検証方法自体は任意である。

【0054】例えば、k行目のコマンド、パラメータ及び実行結果と、k-1行目の認証子Cとについてのハッシュ値をとり、得られたハッシュ値と認証子Cを公開鍵で復号した値が等しいか否かを調べる検証方法や、k行目のコマンド、パラメータ及び実行結果のハッシュ値を得た後、このハッシュ値とk-1行目の認証子Cとの排他的論理和XORをとり、その結果と認証子Cを公開鍵で復号したものが等しいか調べる検証方法などが考えられる。

【0055】ステップST26の検証に基づき、k行目の認証子Cを正当か否かを判定し(ST27)、k行目の認証子Cを正当であると判定したとき、履歴の最後の行まで検証したか否かを判定し(ST28)、最後の行まで検証していない場合には行番号kを1行分増加し(ST29)、ステップST22に戻って同様の操作を繰り返す。なお、ステップST28にて最後の行まで検証した場合には検証処理を終了する。

【0056】一方、ステップST27にて、k行目の認証子Cを正当でないとして判定したとき、警告を発して(ST30)、検証処理を終了する。

【0057】以上により、1行目から最後の行までの履歴に関し、各行の認証子が同一行のコマンド、パラメータ及び実行結果を含んで生成されることから各行毎に改ざんされていない旨と、各行の認証子が直前行の認証子を含んで生々されることから各行の履歴が連鎖している旨とが検証される。但し、図6に示した検証では、最後の行(最新履歴)が削除されたか否かは検証されない。よって、次に、この最新履歴の検証に関して述べる。なお、最新履歴の検証は、前述した履歴の検証において、各行の認証子Cが全て正当と判定された場合に実行される。

【0058】(最新履歴の検証)履歴管理機能25は、図7に示すように、履歴テーブル24Aの最新の行の認証子Cを読出すと共に(ST31)、この認証子CをICカードR/W26を介してICカード30に送る(ST32)。

【0059】ICカード30では、制御機能33がサーバ装置20Aから送られた認証子Cと、最新認証子格納庫31内の最新の認証子Cとを比較し、比較結果をICカードR/W26を経由してサーバ装置20Aの履歴管理機能25に送る(ST33)。

【0060】履歴管理機能25は、比較結果が両認証子Cの同一を示すか否かを判定し(ST34)、判定結果が同一を示すときに処理を終了する。同一でない場合は警告を発し(ST35)、処理を終了する。

【0061】上述したように本実施形態によれば、管理

者の操作履歴に対する各履歴データ(例、コマンド、パラメータ及び実行結果の組)毎に、前回の認証子をも含んで生成した認証子をつけるので、履歴データが改ざんされていない旨と、個々の履歴データの連鎖性を保証でき、もって、管理者による履歴の改ざんを阻止することができる。

【0062】また、最新の認証子の比較結果をも検証するので、最新の認証子の削除に関しても、管理者による履歴の改ざんを阻止することができる。

【0063】また、今回の認証子を生成する際に、以前の履歴を代表するデータとして前回の認証子を用いるので、以前の全ての履歴データを用いて今回の認証子を計算する場合と比べ、ファイルが膨大になることを阻止できると共に、計算量を低下させて認証子の生成速度を向上させることができる。

【0064】なお、本実施形態は、ICカード30内に認証子を格納し、ICカード自体は管理者ですら内容を改ざんできない耐タンパー機構とすることにより、履歴の改ざんを防止している。但し、サーバ装置20AにICカードR/W26を接続することから、ICカード30の管理を厳密にする必要がある。

【0065】(第2の実施形態)図8は本発明の第2の実施形態に係る記憶媒体内のプログラムがインストールされた計算機システムの概略を示す模式図であり、図9はこの計算機システムの構成を示す機能ブロック図である。

【0066】本実施形態は、第1の実施形態の変形例であり、ICカードR/W14を計算機10Aのコマンド発行機能12Aに接続し、この計算機10A側において最新履歴の検証機能を行なう構成となっている。

【0067】コマンド発行機能12Aは、前述したGUI111の操作に基づきコマンド電文を作成する機能に加え、認証子の生成に関する第1の中継機能と、最新の認証子Cの検証に関する第2の中継機能とをもっている。

【0068】コマンド発行機能12Aにおける第1の中継機能は、サーバ装置20Bから受けたレスポンス電文から実行結果を取り出す機能と、この実行結果と、コマンド電文を作成した際のコマンド及びパラメータとをICカードR/W14を経由してICカード30Aに入力する機能と、ICカード30AからICカードR/W14を経由して最新の認証子Cを受けると、この最新の認証子Cを含む認証子電文を生成し、この認証子電文をソケット13経由でサーバ装置20Bに送る機能とから構成されている。

【0069】コマンド発行機能12Aにおける第2の中継機能は、サーバ装置20Bから受けた認証子電文から認証子Cを取り出す機能と、この認証子CをICカードR/W14経由でICカード30Aに入力する機能と、ICカード30AからICカードR/W14経由で受けた比較結果をソケット13経由でサーバ装置20Bに送

る機能とから構成されている。

【0070】履歴管理機能25Aは、前述した機能において、ICカードR/W26に対する送受信に代えて、ICカード30Aに対するコマンド、パラメータ、実行結果及び認証子の送信や最新の認証子の受信を、計算機10Aを介して行なう構成となっている。なお、この履歴管理機能25Aも記憶媒体からプログラムがインストールされることにより実現可能となっている。

【0071】ICカード30Aは、前述した各機能に加え、管理者の認証を行なうための認証機能34を備えている。認証機能34は、ICカード30AがICカードR/W14に挿入されたとき、管理者の操作により、管理者の認証を実行する機能と、この実行結果が管理者の正当な旨を示すとき、履歴管理機能25Aに対して最新履歴の検証を実行させる機能とをもっている。なお、管理者の認証としては、例えばパスワードによる認証といった周知の認証方式が使用可能となっている。

【0072】次に、以上のように構成された計算機システムの動作を図11～図13を用いて説明する。

(管理操作) 始めに、計算機10Aでは、管理者の操作に対し、ICカード30Aの認証機能34を用いて認証を行なう。管理者の認証の後、後述する最新履歴の検証が正常に完了すると、計算機システムは、図11及び図12に示す如き、管理操作が可能となる。

【0073】いま、計算機10Aの管理操作からサーバ装置20Bのコマンド実行までは、図12に示すように、前述同様に実行される(ST1～ST4)。サーバ装置20Bでは、コマンド解釈機能22が、管理機能23の返す実行結果をもとにコマンド解釈機能22においてレスポンス電文を生成し、当該レスポンス電文をソケット21を介して計算機10Aに送信する(ST41)。

【0074】計算機10Aでは、このレスポンス電文をソケット13を経由してコマンド発行機能12Aが受け、コマンド発行機能12Aがレスポンス電文から実行結果を取り出す(ST42)。

【0075】また、コマンド発行機能12Aは、コマンド電文を生成した際のコマンド及びパラメータと、レスポンス電文から取り出した実行結果とをICカードR/W14を経由してICカード30Aに入力する(ST43)。

【0076】ICカード30Aは、これらの入力内容に対し、秘密鍵格納庫32内の秘密鍵による暗号化を施して前述同様に最新の認証子Cを生成し、この最新の認証子Cを最新認証子格納庫31に格納する一方(ST44)、この最新の認証子CをICカードR/W14を介してコマンド発行機能12Aに出力する。

【0077】コマンド発行機能12Aは、ICカード30Aから受けた最新の認証子Cを含む認証子電文を生成し、この認証子電文をソケット13経由でサーバ装置2

0Bに送り返す(ST45)。

【0078】サーバ装置20Bでは、認証子電文をソケット21経由でコマンド解釈機能22にて受け取り、認証子Cを取り出す。

【0079】コマンド解釈機能22は、ステップST4のコマンド、パラメータ及び実行結果と、計算機10Aから受けた最新の認証子Cとを履歴管理機能25Aに送る。履歴管理機能25Aは、これらコマンド、パラメータ、実行結果及び最新の認証子Cを履歴テーブル24Aに書き込んで(ST46)、処理を終了する。

【0080】(履歴の検証) 履歴テーブル24Aの各行毎の認証子Cに対する検証は、第1の実施形態と同様に実行される。この検証の実行タイミングは任意である。

【0081】(最新履歴の検証) 最新の認証子CとICカード30A内の認証子Cの検証について図13のフローチャートを用いて説明する。この検証は、ICカード30Aを管理者が保持するために、任意のタイミングでは実行されない。そこで、この検証は、例えば管理者がサーバ装置20Bにログインした時(認証機能34による認証の直後)といった特定のタイミングに実行される。なお、この検証は、前述した図7に示す検証において、履歴管理機能25AとICカード30Aとの間に計算機10Aを介在させたものである。

【0082】始めに、サーバ装置20Bでは、履歴管理機能25Aが履歴テーブル24Aの最新の行の認証子Cを読み出すと共に(ST51)、この認証子Cをコマンド解釈機能22に与える。コマンド解釈機能22は、この認証子Cを認証子電文の形でソケット21を介して計算機10Aに送る(ST52)。

【0083】計算機10Aでは、認証子電文をコマンド発行機能12Aで受け取り、認証子CをICカード30Aに送る(ST53)。

【0084】ICカード30Aでは、制御機能33がサーバ装置20Aから送られた認証子Cと、最新認証子格納庫31内の認証子Cとを比較し、比較結果をICカードR/W14を経由して計算機10Aのコマンド発行機能12Aに返す(ST54)。

【0085】コマンド発行機能12Aは、比較結果をソケット13を介してサーバ装置20Bに送る(ST55)。

【0086】サーバ装置20Bでは、比較結果を履歴管理機能25Aが受取り、この履歴管理機能25Aが、比較結果について両認証子Cの同一を示すか否かを判定し(ST56)、判定結果が同一を示すときに処理を終了する。同一でない場合は警告を発し(ST57)、処理を終了する。

【0087】この処理が例えばログイン時に行われたとき、計算機10Aは、以後の管理操作が可能となる。

【0088】上述したように本実施形態によれば、ICカード30AをICカードR/W14を介して計算機1

0Aに接続し、計算機10A側において最新履歴の検証を実行させる構成としても、第1の実施形態と同様の効果を得ることができる。

【0089】なお、第2の実施形態は、ICカード30Aを管理者側の管理とし、管理者のシステムへの認証を兼ねている構成である。しかし、計算機10Aとサーバ装置20Bの間の通信が中断した場合、ICカード30A内の最新の認証子Cと、サーバ装置20B側の最新の認証子Cとが不整合となる可能性がある。この場合、履歴改ざんの警告が出されるが、この警告が改ざんによるものか、通信の中断によるものかの判断が困難である。このため、第2の実施形態は、通信上のトラブルの可能性が低い、あるいは別の手段でトラブルが回避できる状況のときに用いることが好ましい。

【0090】尚、本発明における記憶媒体としては、磁気ディスク、フロッピー（登録商標）ディスク、ハードディスク、光ディスク（CD-ROM、CD-R、DVD等）、光磁気ディスク（MO等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【0091】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【0092】さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【0093】また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【0094】尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【0095】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0096】なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。

【0097】例えば、計算機10に代えて、計算機10、10Aと同一構成のコンソール10\*、10A\*をサーバ装置20A、20Bに接続し、このコンソール10

0\*、10A\*からサーバ装置20A、20Bを管理する構成としても、本発明を同様に実施して同様の効果を得ることができる。

【0098】ICカードR/W26は、外付けの態様に限らず、サーバ装置20に内蔵された態様としてもよい。ICカードR/W14も同様に計算機10Aに内蔵されていてもよい。また、ICカード30、30Aは、同様の機能を有し、内部のデータが安全に管理されるデバイス（例、ICカードと同様の機能をもつ回路が形成されたボードなど）に変更してもよく、この場合、ICカードR/W26、14は省略してもよい。

【0099】また、各実施形態は可能な限り適宜組合せて実施してもよく、その場合、組み合わせられた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組合せにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【0100】その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【0101】

【発明の効果】以上説明したように本発明によれば、管理者による履歴の改ざんを阻止し得る履歴管理用の記憶媒体及びICカードを提供できる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る記憶媒体内のプログラムがインストールされた計算機システムの概略を示す模式図

【図2】同実施形態における計算機システムの構成を示す機能ブロック図

【図3】同実施形態における履歴テーブルの構成を示す模式図

【図4】同実施形態におけるICカードの構成を示す機能ブロック図

【図5】同実施形態における動作を説明するためのフローチャート

【図6】同実施形態における動作を説明するためのフローチャート

【図7】同実施形態における動作を説明するためのフローチャート

【図8】本発明の第2の実施形態に係る記憶媒体内のプログラムがインストールされた計算機システムの概略を示す模式図

【図9】同実施形態における計算機システムの構成を示す機能ブロック図

【図10】同実施形態におけるICカードの構成を示す機能ブロック図

【図11】同実施形態における動作を説明するためのシ



## 一ケンス図

【図12】同実施形態における動作を説明するためのフローチャート

【図13】同実施形態における動作を説明するためのフローチャート

【図14】従来の計算機システムの概略を示す模式図

【図15】従来の計算機システムの構成を示す機能ブロック図

【図16】従来の履歴テーブルの構成を示す模式図

【符号の説明】

10, 10A...計算機

11...GUI

12, 12A...コマンド発行機能

13, 21...ソケット

14, 26...ICカードR/W

20A, 20B...サーバ装置

22...コマンド解釈機能

23...管理機能

24A...履歴テーブル

25, 25A...履歴管理機能

30, 30A...ICカード

31...最新認証子格納庫

32...秘密鍵格納庫

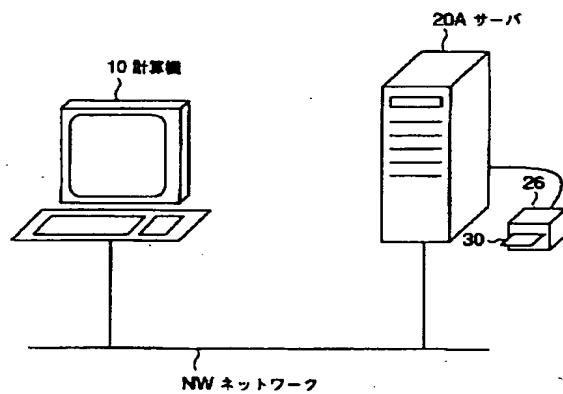
33...制御機能

34...認証機能

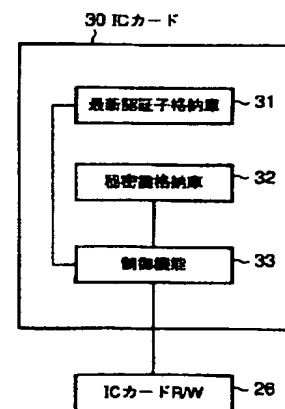
NW...ネットワーク

C...認証子

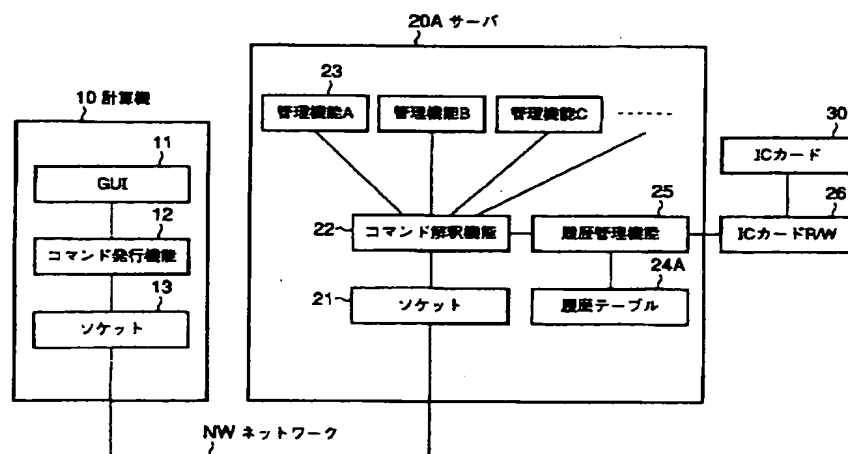
【図1】



【図4】



【図2】



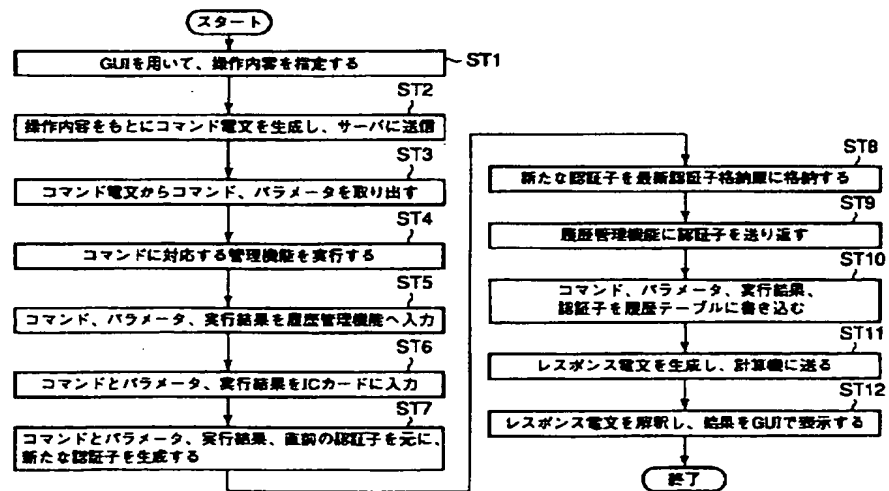
【図3】

24A

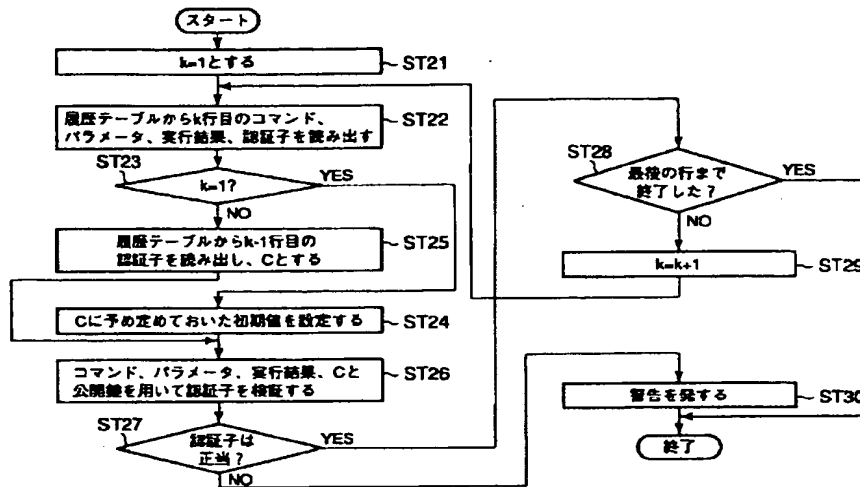
No.	コマンド	パラメータ	実行結果	認証子
1	Port番号設定	80	成功	15AA5BD98
2	タイムアウト時間設定	5秒	成功	4FB35C714
3	ルートディレクトリ変更	c:\www	成功	79E0FA35A
4	...	...	...	
5	...			

C

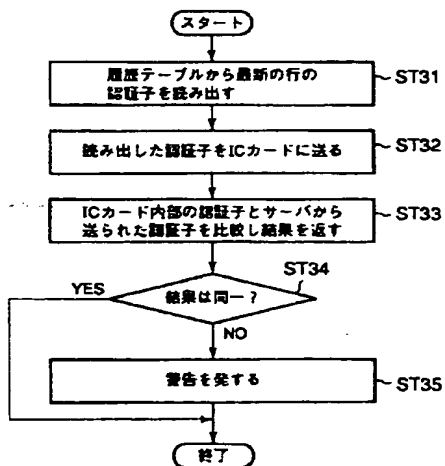
【図5】



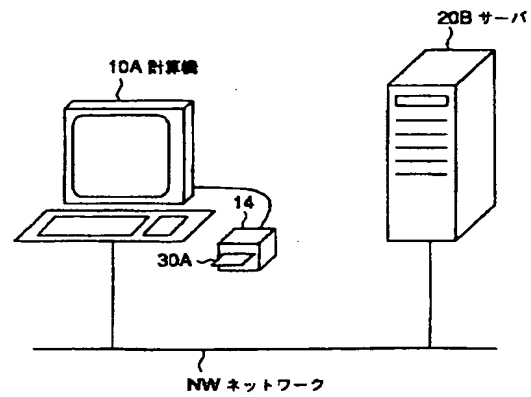
【図6】



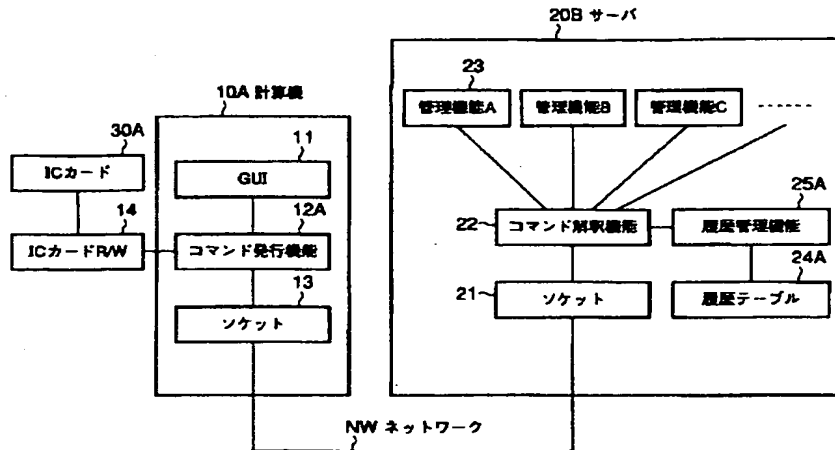
【図7】



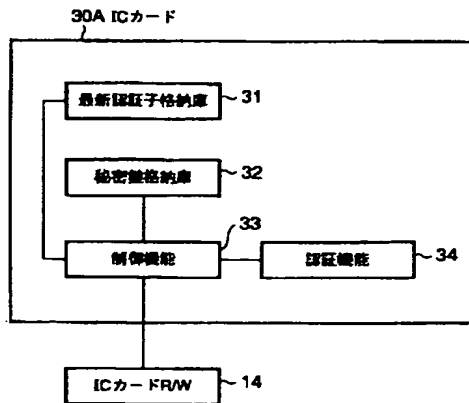
【図8】



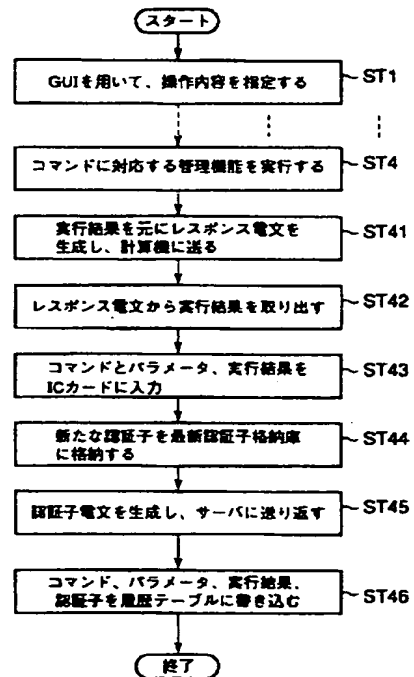
【図9】



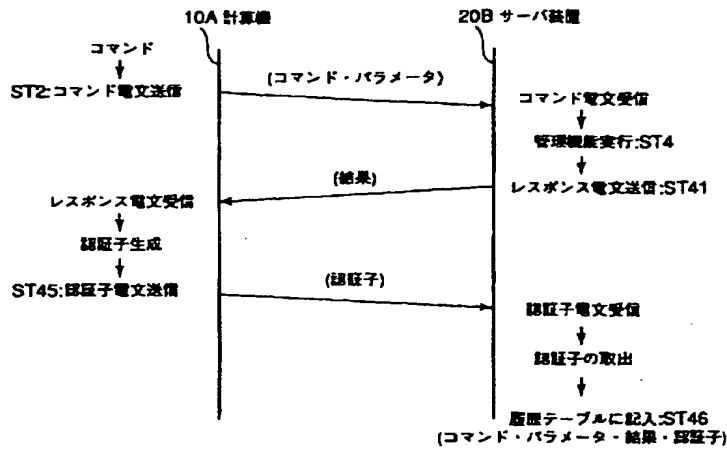
【図10】



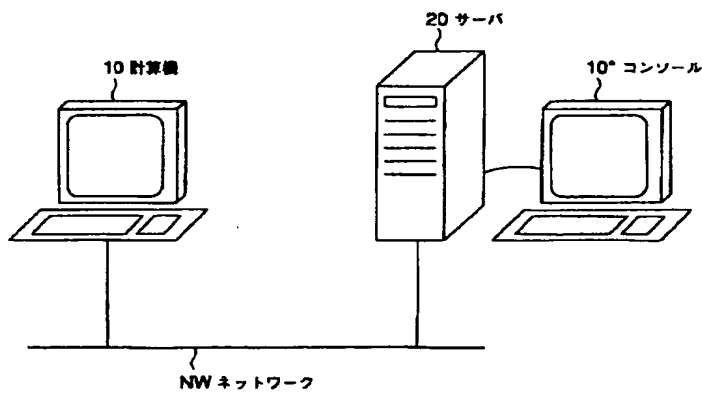
【図12】



【図11】



【図14】

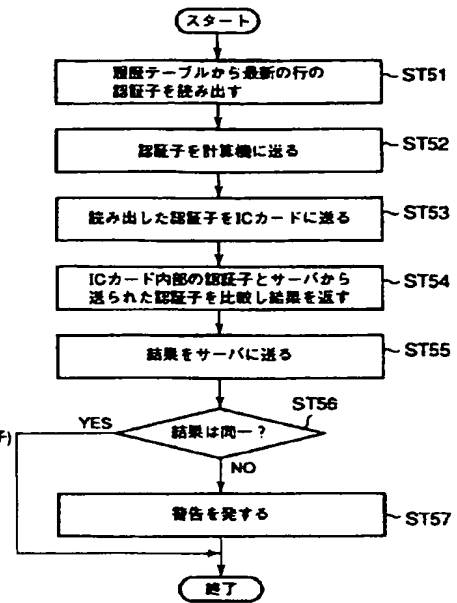


【図16】

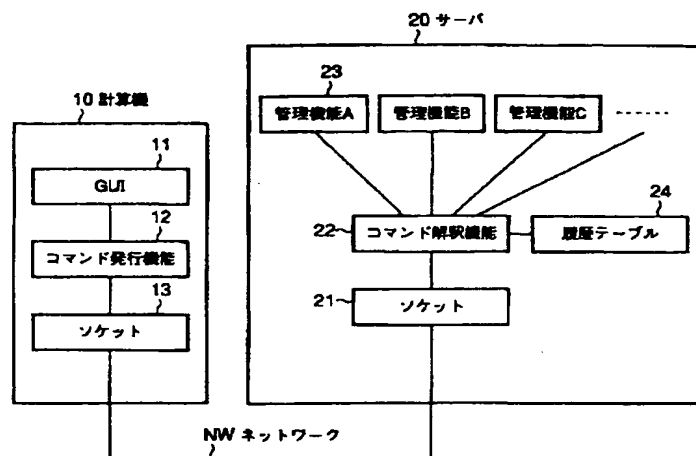
24

No.	コマンド	パラメータ	実行結果
1	Port番号設定	80	成功
2	タイムアウト時間設定	5秒	成功
3	ルートディレクトリ変更	c:\www	成功
4	...	...	
5	...		

【図13】



【図15】



フロントページの続き

F ターム(参考) SB017 AA01 BA06 BB09 CA15 CA16  
 SB035 AA13 BB09 BC00 CA38  
 SB042 JJ08 JJ10 KK13 MA20 MC37  
 MC40  
 SJ104 AA08 BA02 LA03 LA05 NA02  
 NA12 NA31 NA32 NA35 NA37  
 NA38 NA42